



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,511	01/04/2002	Andrew Brown	COMP.0268 P01-3942	6225

7590 03/15/2006
Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER

SHIFERAW, ELENI A

ART UNIT PAPER NUMBER

2136

DATE MAILED: 03/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/037,511

Applicant(s)

BROWN ET AL.

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 December 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the arguments and/or amendments filed on December 27, 2005.

Claim 1 has been amended by the applicant.

Claims 1-20 remain pending and are herein considered.

Response to Arguments

1. Applicant's arguments and/or amendments with respect to amended claim 1, and presently pending independent claims 1, 11 and 17 have been considered but are moot in view of the new ground(s) of rejection.

The applicant's first argument concerns Saarinen, Kara, and Nordqvist failure to disclose *remotely storing a seed pool backup of the seed pool via a network; and restoring the seed pool backup via the network to local memory following a power loss event and/or battery replacement causing loss to the seed pool* as recited in claims 1, 11, and 17. The Examiner respectfully disagrees with the applicant's contentions and would like to draw the Applicant's attention to col. 3 lines 25-55 wherein Kara discloses **a processor-based system or personal computer generating cryptography keys and a touch memory device, utilized as a portable memory device, utilizing to provide seed information for key generation and the touch memory device being physically remote from the processor-based system/PC. It is clear that Kara does in fact teach remotely storing seed value/pool and remotely providing seed value to the processor-based system and processor-based system generating cryptography keys using remotely received seed values** as recited in claims 1, 11, and 17. Examiner would like to draw

the Applicant's attention to paragraph 0023 where in Nordqvist disclose *a backup storage means for storing algorithms and initial values as a backup in a non-volatile memory or battery backed-up RAM memory area to allow lost algorithms and initial values retained/restored, in the event of power loss/interruption*. It is clear that Nordqvist does teach the well-known backup system for data lost, in the event of power-loss as recited in claims 1, 11, and 17. Examiner again would like to draw the Applicant's attention to paragraph 0022 and fig. 5A-B wherein Saarinen discloses **re-seeding at each instance of input entropy in order to change the internal state of the Pseudo-random number generators/PRNGs, in the event of crypto-analytic attacks by which outputs from the PRNG may be guessed or determined, for secure key generation.**

As per Applicant's concerning Examiner's *failure to provide objective evidence, rather than subjective belief and unknown authority, of the requisite motivation or suggestion to combine or modify the cited references*, the Examiner would like to refer to MPEP 2144 wherein **"The rationale to modify or combine the prior art does not have to be expressly stated in the prior art; the rationale may be expressly or impliedly contained in the prior art or it may be reasoned from knowledge generally available to one of ordinary skill in the art,** established scientific principles, or legal precedent established by prior case law. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). See also In re Kotzab, 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000) (setting forth test for implicit teachings); In re Eli Lilly & Co., 902 F.2d 943, 14 USPQ2d 1741 (Fed. Cir. 1990) (discussion of reliance on legal precedent); In re Nilssen, 851 F.2d 1401, 1403, 7 USPQ2d 1500, 1502 (Fed.

Cir. 1988) (references do not have to explicitly suggest combining teachings); Ex parte Clapp, 227 USPQ 972 (Bd. Pat. App. & Inter. 1985) (examiner must present convincing line of reasoning supporting rejection); and Ex parte Levengood, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993) (reliance on logic and sound scientific reasoning).”

As per Applicant’s arguments concerning reference’s failure to teach *periodically storing the seed pool backup on a remote storage device as recited in claims 2, 11, and 17*, the examiner disagrees with the Applicant’s contentions and draws the Applicants attention to paragraph 0022 and fig. 5A-B wherein Saarinen discloses **re-seeding at each instance of input entropy in order to change the internal state of the Pseudo-random number generators/PRNGs, in the event of crypto-analytic attacks by which outputs from the PRNG may be guessed or determined, for secure key generation**. It is very clear that Saarinen does in fact teach periodically storing/re-seeding the seed pool for security to avoid crypto-analytic attacks by which outputs from the PRNG may be guessed or determined. And as examiner addresses above, Nordqvist in paragraph 0023 discloses *a backup storage means for storing algorithms and initial values as a backup in a non-volatile memory or battery backed-up RAM memory area to allow lost algorithms and initial values retained/restored, in the event of power loss/interruption*. Sufficient motivation to combine is provided in the Office Action mailed on 09/27/2005 pages 3-7.

As per Applicant’s arguments concerning reference’s failure to teach *modifying the seed pool backup with additional random bits*, the Examiner would like to draw the Applicant’s attention to pages paragraph 2-3 wherein Saarinen discloses secure PRNGs output relying upon

producing random padding in cryptographic padding mechanisms for unpredictable PRNG outputs of key generation. Padding refers to modifying with additional random bits.

As per Applicant's amendments and argument of claim 1 concerning the references failure to disclose *generating a second random number using the seed pool backup*, the examiner disagrees with Applicant's contentions and would like to refer paragraph 0022 wherein **Saarinen discloses generating a first random number for key generation from a seed value and generating a second random number for a key by re-seeding the PRNG in the event of attack. And also Examiner would like to refer to Moerder USPN 4,634,808 col. 5 lines 1-52 and col. 7 lines 52-68 wherein storage for storing plurality of backup seed values and generating random number key from a seed value and regenerating a second random number key from a stored plurality backup seed value in the event of the random number key is compromised by unauthorized user.** It would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Moerder within the combination system of Saarinen, Kara, and Nordqvist because it would generate a second random number from the seed pool backup to enhance security.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that the system of the prior art, Saarinen, Kara, and Nordqvist do teach or suggest the subject matter as recited in independent claims 1, 11 and 17. Dependent claims 1-10, 12-16 and 18-20 are also rejected at least by virtue of their dependency on independent

claims and by other reason set forth in this office action dated March 8, 2006.

Accordingly, rejections for claims 1-20 are respectfully maintained.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 11, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koza et al. (Koza, USPN 4,652,998) in view of Moerder USPN 4,634,808.

Regarding claims 1, 11, and 17 Koza disclose a method/system of ensuring a random number for a cryptography security subsystem of a processor-based device, and the method/system comprising the acts of:

obtaining a seed pool comprising a plurality of bits for random number generation (col. 2 lines 66-col. 3 lines 1 and col. 11 lines 65-col. 12 lines 6; *central controller comprising a plurality of seed pool bits for random number generation*);

remotely storing a seed pool backup of the seed pool via a network (fig. 1 element 24 and 20, and col. 12 lines 7-31; *seed pools for device 20 are stored remotely in central controller*);
and

transmitting and restoring a periodically stored backup of the seed pool to the security system via a network following loss of the seed pool from the security system (fig. 1 element 24

and 20, col. 6 lines 65-68, and col. 12 lines 7-31; *central controller providing and periodically storing first and new seed pools to terminal controller of the remote devices to generate random number, via a network following key compromization*);

generating a second random number using the seed pool backup (col. 6 lines 65-68, col. 14 lines 36-44, & 16-18, col. 18 lines 63-68, and col. 11 lines 65-31; *plurality of events are occur on terminal device 20/security system i.e. battery power failure, power removal, low power and etc, and terminal device 20 calls/transmits event messages to the remote central controller and the remote central controller processing each event remotely including transmitting a new seed to terminal device 20 via a network so terminal device 20 can regenerate random number key using the new seed and start a new/second pool*).

Koza fails to explicitly disclose the new seed pool transmitted over the network to terminal device is a backup seed.

However Moerder discloses a backup seed pool for random number key generation and providing the backup seed pool in the event of key compromization (fig. 2 element 163, col. 7 lines 52-67 and col. 5 lines 1-52).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Moerder's seed pool backup within the same device to the method/system of remote seed pool backup in the certain device failure events caused by power loss or system outage or compromization because it would provide a new or backup seed to the system that lost the seed pool or compromised key, for security reasons. One would have been motivated to do so because it would keep the key generator processor going

producing key by remotely backing-up/providing new key seeds during power outage/compromization.

4. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saarinen (Pub. No.: US 2002/0172359 A1), in view of Kara (Patent Number: 5,802,175), Nordqvist et al. (Nordqvist, Pub. No.: US 2002/0191799 A1) and Moerder USPN 4,634,808.

As per claim 1, Saarinen teaches a method of ensuring a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of:

obtaining a seed pool comprising a plurality of bits for random number generation (Saarinen page 2 par. 0022 lines 7-10 and par. 0014);

generating a first random number using the seed pool (par. 0007; *seeding a PRNG an initial state/seed to generate random number*)

Saarinen doesn't explicitly teach remotely storing seed pool;

However **Kara** discloses: remotely storing a seed pool via a network (Kara col. 6 lines 3-15, Kara col. 3 lines 51-58 and col. 2 lines 43-46; portable memory device/Touch Memory remotely providing/storing seed values for key generation to PC/processor-based); and

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to remotely seeding starting values to generate session key because it would securely transmit/store seed values remotely through computer network and/or telecommunications for key generation and decryption of data.

Saarinen and Kara fail to explicitly disclose restoring the seed pool backup to local memory following a power loss event causing loss to the seed pool.

However **Nordqvist** discloses restoring the seed pool backup to local memory following a power loss event causing loss to the seed pool (Nordqvist page 2 par. 0023; retaining/restoring/repopulating data/initial value/algorithm stored on RAM/power dependent memory during power interruptions/loss or removal of battery and loss of data).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nordqvist within the combination system of Saarinen and Kara because it is well known to backup a data during battery replacement or power/data loss. One would have been motivated to incorporate the teachings of bucking up data/seed because it would retain/replace the seed data during battery replacement or power interruptions (Nordqvist page 2 par. 0023).

Saarinen, Kara, and Nordqvist fail to explicitly teach generating a second random number using the seed pool backup. However Moerder discloses generating a second random number key from a backup seed values stored (col. 5 lines 1-52 and col. 7 lines 52-col. 8 lines 28).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Moerder key compromising event to power outage and provide a backup seed for random number key generation because it would provide a new backup seed to the random number key generator to generate new second random number key in the event of power outage. One would have been motivated to do so because it would keep the key generator processor going to produce key by remotely backing-up key seeds during power outage.

As per claim 11, Saarinen teaches a method of restoring a seed pool for generating a random number for a security system, the method comprising the acts of:

transmitting a periodically the seed pool to the security system (Saarinen page 4 par. 0071; periodically re-seeding upon each new instance of new input entropy);

seed pool for use in generating the random number (Saarinen page 2 par. 0022 lines 7-10 and fig. 5B element 518);

Saarinen doesn't explicitly teach remotely seeding or storing of seed values remotely;

However **Kara** discloses: transmitting seed pool to the security system via a network (Kara col. 6 lines 3-15, Kara col. 3 lines 51-58 and col. 2 lines 43-46; portable memory device/Touch Memory remotely providing seed values for key generation); and

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to remotely seeding starting values to generate session key because it would securely transmit seed values remotely through computer network and/or telecommunications for key generation and decryption of data.

Saarinen and Kara fail to explicitly disclose repopulating local memory of the security system with the stored backup following loss of the seed pool;

However Nordqvist discloses:

transmitting a periodically stored backup of the seed pool (*initial value or algorithm or data*) to the security system following loss of the seed pool from the security system (Nordqvist page 2 par. 0023; retaining/restoring/repopulating data/initial value/algorithm stored on RAM/power dependent memory during power interruptions/loss or removal of battery and loss of data); and

repopulating local memory of the security system with the stored backup (Nordqvist page 2 par. 0023; retaining/restoring/repopulating data/initial value/algorithm stored on RAM/power dependent memory during power interruptions/loss or removal of battery and loss of data).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nordqvist within the combination system of Saarinen and Kara because it is well known to backup a data during battery replacement or power/data loss. One would have been motivated to incorporate the teachings of backing up data/seed because it would retain/replace the seed data during battery replacement or power interruptions (Nordqvist page 2 par. 0023).

As per claim 17, Saarinen teaches a security system, comprising:

a security subsystem, comprising:

a power dependent memory device (Saarinen page 3 par. 0030);

a limited life battery for the power dependent memory device (Saarinen page 3 par. 0030);

a seed pool stored on the power dependent memory device, wherein the seed pool comprises a plurality of random bits (Saarinen page 2 par. 0014); and

security logic configured to generate a cryptographic key to establish a secure communication session between the electronic device and an external device, wherein the security logic generates the cryptographic key from the seed pool (Saarinen page 1 par. 0002 and page 2 par. 0022 lines 7-10; generation of session key from seed); and

a control module configured for periodically storing the seed pool in the remote storage device (Saarinen page 4 par. 0071; periodically re-seeding upon each new instance of new input entropy);

Saarinen doesn't explicitly teach remotely seeding or storing of seed values remotely;

However **Kara** discloses: a security system, comprising:

a remote storage device (Kara col. 6 lines 3-15, Kara col. 3 lines 51-58 and col. 2 lines 43-46; portable memory device/Touch Memory remotely providing seed values for key generation); and

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to remotely seeding starting values to generate session key because it would securely transmit seed values remotely through computer network and/or telecommunications for key generation and decryption of data.

Saarinen and Kara fail to explicitly disclose backup following replacement of the limited life battery.

However **Nordqvist** discloses a restoration control module configured for repopulating the power dependent memory device with the backup following replacement of the limited life battery (Nordqvist page 2 par. 0023; retaining/restoring/repopulating data/initial value/algorithm stored on RAM/power dependent memory during power interruptions/loss or removal of battery and loss of data).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Nordqvist within the combination system of Saarinen and Kara because it is well known to backup a data during battery replacement or

power loss. One would have been motivated to incorporate the teachings of bucking up data/seed because it would retain/replace the seed data during battery replacement or power interruptions (Nordqvist page 2 par. 0023).

As per claim 2, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition the combination teach the method, wherein the act of remotely storing the seed pool comprises the act of periodically storing the seed pool backup on a remote storage device (Saarinen page 4 par. 0071; periodically **re-seeding upon each new instance of new input entropy** and Kara col. 6 lines 3-15, and col. 2 lines 43-46). The rational for combining are the same as claim 1 above.

As per claims 3 and 14, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition the combination teaches the method wherein the act of periodically storing the seed pool backup comprising the act of periodically storing the seed pool in a remote storage device via the network at an interval based on a write cycle characteristic of the remote storage device to maintain availability of the seed pool as the periodically stored backup (Saarinen page 3 par. 0033 lines 7-10 and Kara col. 6 lines 3-15, and col. 2 lines 43-46). The rational for combining are the same as claim 1 above.

As per claim 4, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition Saarinen teaches the method, comprising the act of modifying the seed pool backup with additional random bits to ensure randomness for generating the random number

(Saarinen page 1-par. 0003 and par. 0007-0008).

As per claim 5, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition Saarinen teaches the method, wherein the act of modifying the seed pool backup with additional random bits comprises the act of capturing one or more bits of data from a free-running timer (Saarinen page 1 par. 0003 lines 5-7 and par. 0007-0008).

As per claims 6 and 13, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition Saarinen teaches the method, wherein the act of modifying the seed pool backup with additional random bits comprises the act of capturing one or more bits of data from a local hardware device (Saarinen page 2 par. 0014).

As per claim 7, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition the combination teaches the method, wherein the act of restoring the seed pool backup comprises the act of automatically retrieving the seed pool backup via the network upon restoring power to the cryptographic security subsystem (Nordqvist page 2 par. 0023, and Kara col. 6 lines 3-15, and col. 2 lines 43-46). The rationale for combining are the same as claim 1 above.

As per claim 8, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition the combination teaches the method, wherein the act of automatically retrieving the seed pool backup comprises requesting the seed pool backup from a remote management

system (Kara col. 6 lines 3-15, and col. 2 lines 43-46 and Nordqvist page 2 par. 0023). The rational for combining are the same as claim 1 above.

As per claim 9, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition Nordqvist teaches the method, wherein the power loss event is a battery failure resulting in memory loss of the seed pool from the local memory (Nordqvist page 2 par. 0023). The rational for combining are the same as claim 1 above.

As per claim 10, Saarinen, Kara, Nordqvist, and Koza teach all the subject matter as described above. In addition the combination teach the method, wherein the act of restoring the seed pool backup comprises the act of transmitting the seed pool backup from remote storage to the local memory via the network following a battery replacement for the local memory (Saarinen col. 3 lines 1-57, Nordqvist page 2 par. 0023, and Kara col. 3 lines 51-58). The rational for combining are the same as claim 1 above.

As per claim 12, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, Saarinen teaches the method, comprising the act of modifying the periodically stored backup with additional random bits to ensure randomness (Saarinen page 1-par. 0003 and par. 0007-0008).

As per claim 15, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, Nordqvist teaches the method, wherein the act of transmitting the periodically stored

backup comprises the act of transferring the periodically stored backup to the security system after restoring battery power to the security system (Nordqvist page 2 par. 0023). The rational for combining are the same as claim 11 above.

As per claim 16, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, the combination teach the method, wherein the act of transferring the periodically stored backup comprises automatically initiating a seed pool restoration event using the periodically stored backup stored on a remote server after restoring battery power by replacing a battery for the local memory of the security system (Nordqvist page 2 par. 0023, and Kara col. 3 lines 51-57). The rational for combining are the same as claim 11 above.

As per claim 18, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, Kara teaches the system, comprising a remote security interface configured for interacting with the security subsystem and the security backup system (Kara col. 2 lines 46-52, and col. 3 lines 51-57). The rational for combining are the same as claim 17 above.

As per claim 19, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, the combination teach the system, wherein the security backup system comprises a seed pool modification module configured for capturing one or more bits of data from a hardware component and adding the one or more bits to the backup (Saarinen 0002-0003, 0035-0038 and Nordqvist page 2 par. 0023). The rational for combining are the same as claim 18 above.

As per claim 20, Saarinen, Kara, and Nordqvist teach all the subject matter as described above. In addition, Nordqvist teaches the system, wherein the security backup system comprises an automation module configured for automatically initiating repopulation of the memory device with the backup (Nordqvist page 2 par. 0023). The rationale for combining are the same as claim 18 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. USPN 5,539,682: Jain et al. discloses seed pool padding.
 USPN 5,237,432: Calaro et al. discloses seed pool padding.
 USPN 5,954,582: Zach discloses remotely storing seed pool to remote devices.
 USPN 6,533,664 B1: Crumby discloses remotely storing seed pool to remote devices.

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Art Unit: 2136

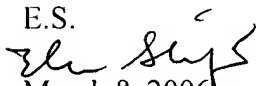
will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

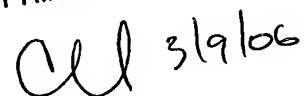
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.


March 8, 2006

CHRISTOPHER REVAH
PRIMARY EXAMINER

 3/9/06